Protect your smartphone

1. Select an access code for your device that consists of at least 6 digits or uses fingerprint or facial recognition. This way, if someone finds or steals your smartphone, they won't have access to your data.
2. Make sure your smartphone and applications are always up to date. Do you have any questions about performing updates? Run updates as soon as you can. Turn off your smartphone regularly. Some updates are performed automatically when you reboot.
3. Only download applications from official app stores: the App Store if you use an iPhone, the Google Play Store if you use another brand of device.
4. Beware of fake text or WhatsApp messages. They look like they come from a company or public service (bank, Itsme®, pension service,...) or promise you a bonus, and they encourage you to click on the links they contain to get your bank codes to empty your accounts. Always be careful if you receive messages from a number you don't know.
5. Use antivirus software for your device.

Protect your computer

1. Learn to identify suspicious messages. Many of the emails you receive are attempted scams. Always think twice if you receive a message from a stranger and never click on a link in a suspicious message.
2. Install antivirus software on your computer.
3. Update your operating system and software regularly.
4. Protect your computer and accounts (e.g., email, Facebook) with a password that is at least 13 characters long. Use different passwords.
5. Have you heard of the two-factor authentication (2FA)? This system is straight-forward and very safe. You can use it protect your important accounts with a double lock. In addition to a password, you use a second key, for example a code that is sent to you by text.

Don't be fooled by calls

1. If you receive a call from a number you don't recognize, always be on your guard.
2. Never give out personal details, passwords, credit card codes or answer codes during a phone call.
3. Never call back unknown numbers. Never answer calls from unknown numbers. Do not call back. If someone needs you, they will leave a message.
4. Don't believe what you hear on the phone straight away. Microsoft or any other tech company will never call you. Your bank will never ask you for your codes or to open a new account by phone.
5. Store the numbers of people you know. Block the numbers of unwanted callers.

What else can you do?

Checklist

✓Never give out personal information, passwords, credit card codes or response codes via email, phone call, text message or social media.

✓I download the Safeonweb application to be alerted to new forms of online scams and follow the advice of the safeonweb.be website.

✓Set an access code on my smartphone.

✓Set up automatic updates on smartphones/ computers.

✓Install an antivirus on your smartphone and computer, if you haven't already done so.

✓Store the numbers of friends and family in your smartphone. Also store the numbers of your bank and other companies that you need to contact often or that may contact you.

✓Protect your mailbox using the two-factor authentication (2FA).

✓Protect your other accounts (Facebook, Instagram,...) with the two-factor authentication (2FA), when possible.

Ask for help!

Not sure where to get started with these tips? Are you in doubt about a message you received? Did you notice anything strange about your computer? Don't stay in doubt! Ask friends or family who have more experience to help.

Do you need more information?
Take a look at www.safeonweb.be and our brochure "Cyber attacks and online scams".
Download our Safeonweb app to be notified of the latest threats.

Safeonweb

Have you received a suspicious email or message?

Send it to suspicious@safeonweb.be and then delete it. You will not receive a personal reply to this email. The links in the e-mail will be blocked, to protect less cautious Internet users.

Point of contact

Are you a victim of a scam, fraud or phishing?

File a report via pointdecontact.belgium.be of the FPS Economy.
You will always get a reply to your report. The competent services will analyse the report and possibly conduct an investigation.

The Centre for Cybersecurity Belgium

Safeonweb is a service of the Centre for Cybersecurity Belgium.

CENTRE FOR CYBER SECURITY BELGIUM

Safeonweb.be

.be

RE : Miguel De Bruycker, Rue de la Loi 18, 1000 Bruxelles

How to outsmart a phisher?

Here are 3 x 5 tips to protect yourself

Safeonweb.be